SYSTEM NAME AND NUMBER: Enterprise Mass Warning and Notification System (EMWNS), DCIO 02 DoD. (March 30, 2020; 85 FR 17545)

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Defense Information System Agency (DISA), 8705 Industrial Boulevard, Tinker Air Force Base, OK 73145-336; Space and Naval Warfare Systems Center, 53560 Hull Street, San Diego, CA 92152-5001; and DoD Azure Cloud environment, 9 Eglin St, Hanscom Air Force Base, MA 01731-2100.

SYSTEM MANAGER(S): Emergency Management Action Officer, Headquarters, Department of the Army, 400 Army Pentagon, Washington, DC 20310-0400.

Program Manager, C3I Infrastructure Division, Hanscom Air Force Base, MA 01731-2100, (781) 225-4319, aflcmc.hnii.EMWNS@us.af.mil.

Commander, Navy Installations Command, 716 Sicard Street SE Building 111, Washington Navy Yard, DC 20388-0001.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 10 U.S.C. 113, Secretary of Defense, 5 U.S.C. 7902, Safety Programs; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; DoDD 5124.02, Under Secretary of Defense for Personnel and Readiness (USD (P&R); DoDI 3020.42, Defense Continuity Plan Development; DoDI 3020.52, DoD Installation Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive (CBRNE) Preparedness Standards; DoD Instruction 6055.17, DoD Emergency Management (EM) Program.

PURPOSE(S) OF THE SYSTEM: An overarching part of the DoD mission is to ensure the protection and safety of DoD personnel and DoD affiliated personnel. The EMWNS is a robust communication system that provides text and voice notifications to both hard-wired and electronic devices. The system integrates with DoD installation Giant Voice loudspeakers to broadcast sound alerts. The EMWNS is an enterprise solution for the DoD to notify and receive accountability information from personnel during emergencies. Additionally, the system supports a "duress" function through the mobile application. This function provides specific users, such as DoD recruiters, a means to alert local command and control units of safety threats.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Active Duty, Reserve, and National Guard personnel, dependents, DoD civilians, and contractors.

CATEGORIES OF RECORDS IN THE SYSTEM: Name, DoD ID Number, Grade/Rank, Office/unit name, physical office location (building number), phone numbers (work, home, and mobile), and email addresses (work and personal). If the mobile application is downloaded and location data is turned on, Global Positioning System (GPS) data will be temporarily collected and stored when a user initiates the duress function.

RECORD SOURCE CATEGORIES: Individuals.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C 552a(b) of the Privacy Act of 1974, as amended, the records contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

a. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government when necessary to accomplish an agency function related to this System of Records.

b. To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.

c. To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.

d. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

e. To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

f. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

g. To appropriate agencies, entities, and persons when (1) the DoD suspects or confirms a breach of the System of Records; (2) the DoD determines as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

h. To another Federal agency or Federal entity, when the DoD determines information from this System of Records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the

risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Paper and electronic.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: The system will retrieve data to send alerts to specific devices. GPS locator data may be collected when a user institutes a duress alert and only during that specific emergency event.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: EMWNS GPS Data: Destroy immediately after the notification.

EMWNS locator or personnel data (cards, machine listings, rosters and comparable data): Destroy when no longer needed.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: Appointed and trained operators may access the system data. Access to the records is limited to person(s) responsible for servicing the records in performance of their official duties. These responsible individuals are properly screened and have a need-to-know of the system information. Records are stored in encrypted databases and are only accessible on DoD networks. The system uses Secured Sockets Layer (SSL) with Public Key Infrastructure (PKI) certificates in the data transfer protocols for encryption. Access to computerized data is restricted by Common Access Card (CAC). In addition, data is encrypted at rest and in transit. Authorized system operators with CACs may access the underlying system application. CAC authentication is required for users (recipients of notifications) to update their contact information and other personal data via a desk top computer. Users may only access their own data and may not access or see other individuals' data.

RECORD ACCESS PROCEDURES: Individuals seeking access to information about themselves contained in this System of Records should address written inquiries to the Office of the Secretary of Defense/Joint Staff Freedom of Information Act Request Service Center, 1150 Defense Pentagon, Washington, DC 20301-1150. For verification purposes, individuals should provide their full name, DoD ID Number, System of Records Notice identification number, and any details which may assist in locating records and their signature. In addition, the requester must provide a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:

If executed outside the United States: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature)."

If executed within the United States, its territories, possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)."

CONTESTING RECORD PROCEDURES: The DoD rules for accessing records, contesting contents, and appealing initial agency determinations are contained in 32 CFR part 310, or may be obtained from the system manager.

NOTIFICATION PROCEDURES: Individuals seeking to determine whether information about themselves is contained in this System of Records at any AF installation should address written inquiries to the Office of the Secretary of Defense/Joint Staff Freedom of Information Act Requester Service Center, 1150 Defense Pentagon, Washington, DC 20301-1150. In addition, the requester must provide either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:

If executed outside the United States: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature)."

If executed within the United States, its territories, possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)."

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: May 1, 2014, 79 FR 24688.